DETAILED ACTION

1. Claims 1-12 are presented for examination.

Priority

2. This application is related to and claimed the benefits of Japan Patent application No.2004-016006 filed January 23, 2004.

Drawings

3. The drawings filed on 07/24/2006 are accepted.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 07/24/2006 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Claim Objections

5. Claims 5, 7, 8, 9 objected to under 37 CFR 1.75(c) as being in improper form because Claims 5, 7, 8, 9 depend on other multiple dependent claims 3, 5, 6. See MPEP § 608.01(n).

Claim 5, recites" the group signature system of claim 3 or 4 ". Claim 3 is a multiple dependent claim itself. A multiple dependent claim should not depend on another multiple dependent claim. Therefore, Claim 5 is in improper form. For examination purposes, it is assumed that claim 5 depends on claim 3.

Claim 7, recites" the group signature system of any one of claim 1 to 6 ". Claims 3, 5, and 6 are multiple dependent claims itself. A multiple dependent claim should not

depend on another multiple dependent claim. Therefore, Claim 7 is in improper form. For examination purposes, it is assumed that claim 7 depends on claim 2.

Claim 8, recites" the group signature system of any one of claim 1 to 6 ". Claims 3, 5, and 6 are multiple dependent claims itself. A multiple dependent claim should not depend on another multiple dependent claim. Therefore, Claim 8 is in improper form. For examination purposes, it is assumed that claim 8 depends on claim 2.

Claim 9, recites" the group signature system of any one of claims 3, 6, 7, or 8 ". Claim 3, 7 and 8 are multiple dependent claims itself. A multiple dependent claim should not depend on another multiple dependent claim. Therefore, Claim 9 is in improper form. For examination purposes, it is assumed that claim 9 depends on claim 8.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 10 are rejected under 35 U.S.C. 102(b) as being anticipated by Hopkins et al (US 2003/0120931 A1) hereinafter Hopkins.

As for claim 1:

Hopkins discloses a group signature system which creates a group signature **(see Hopkins [0013] "a system and method for generating a group digital signature wherein each member of a group of authorized individuals must sign a message**

M to create a group digital signature S. ") to prove that the signer is really a member registered in the group and which confirms whether or not said signer of said group signature thus created is really a member of said group, **(see Hopkins [0004] "the signer somehow endorses the information to communicated by the document ")** comprising:

a group management device which discloses public information for common use throughout the system, in a referenceable manner from other devices, **(see Hopkins [0007] "the public key which is used to verify the digital signature. If many people need to verify a signer's digital signature, the associated public key must be available. A public key may be published or held in an on-line repository or directory where it is easily accessible. Although the public and private keys are mathematically related, it is extraordinarily difficult to derive the private key from knowledge of the public key.")**

a signature device which creates, from a member certificate containing a first element and a second element, encrypted data by encrypting said first element through use of a first random number and said public information disclosed by said group management device; creates first converted data by converting said first element through use of a second random number and said public information; creates second converted data by converting the first element through use of a third random number and the public information; **(see Hopkins [0017] "generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message,**

0 <=M< =n-1, n is a composite number formed from the product of a number k of distinct random prime factors $p_1.p_2.. . . . ..p_k$, k is an integer greater than 2, and $S= M^d(mod\ n)$. ") creates knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, **(see Hopkins [0014] "generating a group digital signature wherein each of the group of individuals sign the message M using a unique individual private key that is not known or accessible to other members of the group. ")** said first element, and said second element; and outputs as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message; **(see Hopkins [0017] "the method includes the steps of: a first individual in a group performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1; at least a second individual in the group performing a second partial digital signature subtask on the message M using a second individual private key to produce a second partial digital signature S_2; and combining the partial digital signature results including the results S_1 and S_2 to produce the group digital signature S corresponding to the message M.")** and

a verification device that verifies whether said group signature has duly been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, based on said message and

said group signature outputted from said signature device and said public information disclosed by said group management device. **(see Hopkins [0006] "Digital signatures may be created and verified by cryptography. Digital signatures commonly use public key cryptography, which employs an algorithm using two different but mathematically related keys; one for creating a digital signature or encoding data, and another key for verifying a digital signature or decoding the message.")**

As for claim 10:

Hopkins discloses a group signature method for a group signature system**(see Hopkins [0013] "a system and method for generating a group digital signature wherein each member of a group of authorized individuals must sign a message M to create a group digital signature S. ")** having a group management device, a signature device and a verification device, which creates a group signature to prove that the signer is really a member registered in the group and which confirms whether or not said signer of said group signature thus created is really a member of said group, **(see Hopkins [0004] "the signer somehow endorses the information to communicated by the document ")** comprising the steps of:

said group management device disclosing public information for common use throughout the system, in a referenceable manner from other devices; **(see Hopkins [0007] "the public key which is used to verify the digital signature. If many people need to verify a signer's digital signature, the associated public key must be available. A public key may be published or held in an on-line repository or**

directory where it is easily accessible. Although the public and private keys are mathematically related, it is extraordinarily difficult to derive the private key from knowledge of the public key.")

said signature device storing a member certificate consisting of a first element and a second element, creating encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device, **(see Hopkins [0017] "generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, 0 <=M< =n-1, n is a composite number formed from the product of a number k of distinct random prime factors $p_1.p_2.. . . . ..p_k$, k is an integer greater than 2, and $S= M^d(\text{mod } n)$. ")** creating first converted data by converting said first element using a second random number and said public information, creating second converted data by converting said first element using a third random number and said public information; creating knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, **(see Hopkins [0014] "generating a group digital signature wherein each of the group of individuals sign the message M using a unique individual private key that is not known or accessible to other members of the group. ")** said first element, and said second element, in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been

created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged, and outputting as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message **(see Hopkins [0017] "the method includes the steps of: a first individual in a group performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1; at least a second individual in the group performing a second partial digital signature subtask on the message M using a second individual private key to produce a second partial digital signature S_2; and combining the partial digital signature results including the results S_1 and S_2 to produce the group digital signature S corresponding to the message M.")**, and

said verification device verifying whether or not said group signature has been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, based on said message and said group signature outputted from said signature device and said public information disclosed by said group management device without using the information concerning said first and second elements and said signature key. **(see Hopkins [0006] "Digital signatures may be created and verified by cryptography. Digital signatures commonly use public key cryptography, which employs an algorithm using two different but mathematically related keys; one for creating a digital signature or**

encoding data, and another key for verifying a digital signature or decoding the message.")

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins as applied to claims 1 above, further in view of Terao et al (US 2001/0009026 A1), hereinafter Terao.

As for claim 2:

Hopkins discloses the group signature system of claim 1, but does not disclose wherein said signature device creates said knowledge signature data in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged; and said verification device verifies whether said group signature has been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, without using information concerning said first element, said second element, and said signature key.

However, Terao disclose wherein said signature device creates said knowledge signature data in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value and that information concerning said first element, said second element, and said signature key will not be divulged; **(see Terao [0051] "The proof data verification device 10 sends the authentication data 14 to the proof data generation device 11. The signature data generation means 15 and the presignature data generation means 16 in the proof data generation device 11 generate proof data (signature) from the received authentication data 14 and both the user unique identifying information (unique information for identifying the user) 17 and the access ticket 18 held in the proof data generation device 11, and sends the proof data thus generated back to the proof data verification device 10. The verification means 13 in the proof data verification device 10 verifies the signature, and if the verification is successful, the execution of program is permitted. ")** and said verification device verifies whether said group signature has been created by using the first and second elements contained in the member certificate of one of the registered members in said group and said signature key, without using information concerning said first element, said second element, and said signature key. **(see Terao [0055] "The proof data generation device 11 (constituted by both a program on a PC or a work station and an IC card) performs calculation on the basis of both user unique identifying information 17 and access ticket 18 and communicates with the proof data verification device 10 on the basis of the calculation. The user**

unique identifying information 17 is used in the course of this calculation, but if the information 17 leaks to the exterior, there arises a problem, so it is necessary that at least a part of the above program be protected by a defensive means such as an IC card or the like.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include the signature key (access ticket) as taught by Terao because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Terao in Hopkins so as not to permit stealing even by the user who is the legitimate holder thereof and that a proof hardware (e.g. IC card or board) having an anti-tamper characteristic be used.

Claims 3, 4, 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins, further in view of Miyaji (US 6697946 B1), hereinafter Miyaji.

As for claim 3:

Examiner notes: Claim 3 recites "the group signature system of claim 1 or 2". For examination purposes, it is assumed that claim 3 depends on claim 1.

Hopkins discloses the group signature system of claim 1, but does not disclose the group signature system of claim 1 or 2, further comprising a member management device which, when registering a new member into said group, selects a member registration private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member registration private key; obtains a member registration public key, which is a generator of a multiplicative

group on a finite field, from said member registration private key; notifies said member registration public key as public information to said group management device; stores said member registration private key in itself; and creates a member certificate using such member registration private key and notifies the resultant member certificate to said signature device.

However, Miyaji discloses group signature system of claim 1 or 2, further comprising a member management device which, when registering a new member into said group, selects a member registration private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member registration private key; obtains a member registration public key, which is a generator of a multiplicative group on a finite field, from said member registration private key; notifies said member registration public key as public information to said group management device; stores said member registration private key in itself; and creates a member certificate using such member registration private key and notifies the resultant member certificate to said signature device**. (see Miyaji column 4 lines 15-34 "a message recovery signature apparatus for signing a message m with a secret key x_A using a discrete logarithm problem as a basis for security, based on operations performed on a finite field GF(p) where p is a prime number and g is an element whose order is q, the message recovery signature apparatus including: a random number generating unit for generating a random number k; a commitment generating unit for generating a commitment r_1 from the random number k according to a function $f_{11}(k)=g^k$; a message masking unit for**

generating a masked message r_2 from the commitment r.sub.1 and the message m according to a function f_{12} (r_1,m) that maps GF(p)xGF(p) into the finite field GF(p); and a signature generating unit for generating a signature s from the masked message r.sub.2 and the secret key x_A according to a function f_{13} (r_2, x_A) the message recovery signature apparatus being characterized in that the function f.sub.12 (r.sub.1,m) has a property that when g^{xA} denotes a public key y^A and t, j, and e denote elements of a finite ring Zq=[0, 1, . . . , q-1], the three variables t, j, and e are unable to be replaced with two algebraic relations in f_{12} (g^t y_A^j,my $_A^e$) and f_{12} (g^t y_A^j,mg $_A^e$).")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include the key be a generator of finite field of a prime number as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with higher secured condition so to avoid the forger to attack the system.

As for claim 4:

The combination of Hopkins and Miyaji discloses the group signature system of claim 3, wherein said member certificate is a Nyberg-Rueppel signature which uses said signature key as a discrete logarithm and which is created by using said member registration private key on the converted data from said signature key. **(see Miyaji column 1 lines 13-15 "Nyberg-Rueppel proposes a message recovery signature**

scheme which is carried out by a public key cryptosystem using the discrete logarithm problem as a basis for security. ")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include Nyberg-Rueppel signature as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with discrete logarithm over a finite field so to avoid the forger to attack the system.

As for claim 5:

Examiner notes: Claim 5 recites "the group signature system of claim 3 or 4". For examination purposes, it is assumed that claim 5 depends on claim 3.

The combination of Hopkins and Miyaji discloses the group signature system of claim 3 or 4, wherein said group management device discloses, in addition to said public information, said member information notified by said member management device in a referenceable manner from other devices. **(see Miyaji column 15 lines 40-50 "The public key announcing unit 14 announces the generated public key to all users in the system together with the user name corresponding to the public key. Here, if an inquiry is made by any of the users in the system, the public key announcing unit 14 accordingly announces a required user name and its public key among public keys generated in the management center 1 for users in the system. The secret key notification pattern generating unit 15 protects**

secret keys of the users in the system from being accidentally revealed due to misoperations.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include notification as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with notification function so to avoid the forger to attack the system.

Claims 6, 7, 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins and Terao as applied to claim 2 above , further in view of Miyaji (US 6697946 B1), hereinafter Miyaji.

As for claim 6:

Examiner notes: Claim 6 recites "the group signature system of claim 1 or 2". For examination purpose, it is assumed that claim 6 depends on claim 2.

The combination of Hopkins and Terao does not disclose the group signature system of claim 1 or 2, further comprising a plurality of member sub-management devices which, when registering a new member into said group, assigns one of the distributed values for obtaining the required generator of a finite field having the order of a prime number as its own distributed member registration private key; stores said distributed member registration private key in itself; and uses as a member registration public key the value having said generator as a discrete logarithm; and wherein said signature device obtains a member certificate by communicating with a plurality of said member sub-

management devices, and said group management device acquires said member registration public key.

However, Miyaji discloses the group signature system of claim 1 or 2, further comprising a plurality of member sub-management devices which, when registering a new member into said group, assigns one of the distributed values for obtaining the required generator of a finite field having the order of a prime number as its own distributed member registration private key; stores said distributed member registration private key in itself; and uses as a member registration public key the value having said generator as a discrete logarithm; **(see Miyaji column 11 lines 45-49 " The message recovery signature scheme in this system is a public key cryptosystem that uses the discrete logarithm problem as the founding principle for the security, and is based on operations over an elliptic curve E(GF(p)) defined on a finite field GF(p) where p is a prime number. ")** and wherein said signature device obtains a member certificate by communicating with a plurality of said member sub-management devices, **(see Miyaji column 11 lines 38-41 "FIG. 6 shows the message recovery signature algorithm and data exchange between the three parties (user A 510, management center 520, and user B 530) ")** and said group management device acquires said member registration public key. **(see Miyaji column 12 lines 21-32 "First, the management center 520 uses the user A's secret key x_A which has been informed by the user A 510 beforehand (S570) to generate a public key y_A of the user A 510 according to $y_A = x_A G$**

The management center 520 then reveals the system parameters

(p, E, G, ha, hb, hc) to the user A 510 and user B 530, as well as informing the user B 530 of the user A's public key y_A (S572 and S573).")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the modified-invention of Hopkins to include discrete logarithm over a finite field with public key as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with discrete logarithm over a finite field with public key so to avoid the forger to attack the system.

As for claim 7:

Examiner notes: Claim 7 recites "the group signature system of any one of claims 1 to 6". For examination purposes, it is assumed that claim 7 depends on claim 2.

The combination of Hopkins and Terao does not disclose the group signature system of any one of claims 1 to 6, further comprising a member tracking device which selects a member tracking private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member tracking private key; obtains a member tracking public key that is a generator of a multiplicative group on a finite field from said member tracking private key; notifies said member tracking public key as said public information to said group management device; stores said member tracking private key in itself; when identifying the signer of a group signature, decrypts the encrypted data contained in said group signature by using said member tracking private key; and, if the result of decryption matches the first element of one of

said member certificates which have been disclosed by said group management device, identifies the member of such member certificate as the signer; and wherein said group management device has disclosed said member certificate as said member information; and when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information.

However, Miyaji discloses the group signature system of any one of claims 1 to 6, further comprising a member tracking device which selects a member tracking private key so that the key will be a generator of a finite field having the order of a prime number; uses a discrete logarithm as said member tracking private key; obtains a member tracking public key that is a generator of a multiplicative group on a finite field from said member tracking private key; notifies said member tracking public key as said public information to said group management device; stores said member tracking private key in itself; when identifying the signer of a group signature, decrypts the encrypted data contained in said group signature by using said member tracking private key; and, if the result of decryption matches the first element of one of said member certificates which have been disclosed by said group management device, identifies the member of such member certificate as the signer; and wherein said group management device has disclosed said member certificate as said member information. **(see Miyaji column 5 lines 56-67 "FIG. 1 shows the configuration of the first embodiment of a products trading system that uses a message recovery signature apparatus of the present invention. This system includes a management center 520 which manages communications for products trading, a user A 510 as an orderer of**

products, a user B 530 as a seller of the products, and a public network 540 which connects the management center 520 and the users in the system. In this system, message recovery signatures by encryption are used to place orders for products in order to ensure safe products trading. ") and when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information. **(see Miyaji column 1 lines 35-42 ""Public key cryptosystem" is a cryptosystem that uses different keys for encryption and decryption, with the decryption key being kept secret and the encryption key being made public. Public key encryption provides a convenient method for managing the separate encryption keys of many users, and so has become a fundamental technique for performing communications with a large number of users.")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the modified-invention of Hopkins to include Public key cryptosystem as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with Public key cryptosystem so to avoid the forger to attack the system.

As for claim 8:

Examiner notes: Claim 8 recites "the group signature system of any one of claims 1 to 6". For examination purpose, it is assumed that claim 8 depends on claim 2.

The combination of Hopkins and Terao does not disclose further comprising a plurality of member sub-tracking devices, wherein the distributed member tracking private key for each member sub-tracking device is the one to be assigned to itself, among the distributed values for obtaining the generator of a finite field having the order of a prime number; and each of which obtains said distributed member tracking private key so that the member tracking public key has a discrete logarithm as the generator of said finite field and will be a generator of a multiplicative group on a finite field; and each of which stores said distributed member tracking private key in itself; when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information; said group management device has disclosed said member certificate as said member information; and during the process of identifying the signer of a group signature, each of said member sub-tracking devices identifies the member of one of said member certificates as the signer, if the decryption result obtained from the result of performing a pre-determined calculation on the encrypted data contained in said member group signature.

However, Miyaji discloses the group signature system of any one of claims 1 to 6, further comprising a plurality of member sub-tracking devices, wherein the distributed member tracking private key for each member sub-tracking device is the one to be assigned to itself, among the distributed values for obtaining the generator of a finite field having the order of a prime number; and each of which obtains said distributed member tracking private key so that the member tracking public key has a discrete logarithm as the generator of said finite field and will be a generator of a multiplicative

group on a finite field; and each of which stores said distributed member tracking private key in itself; when creating said encrypted data by encrypting said first element, said signature device uses said member tracking public key as said public information; said group management device has disclosed said member certificate as said member information; and during the process of identifying the signer of a group signature, each of said member sub-tracking devices identifies the member of one of said member certificates as the signer, if the decryption result obtained from the result of performing a pre-determined calculation on the encrypted data contained in said member group signature **(see Miyaji column 7 lines 52-55 "The system parameters (p, q, g, f, ha, hb, hc) that define the above system conditions have been stored in the system parameter storing unit 523 in the management center 520 in advance.")** by using each of their said distributed member tracking private keys matches the first element of one of said member certificates that have been disclosed by said group management device. **(see Miyaji column 7 lines 14 to column 8 lines 7 for < system conditions> paragraph)**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the modified-invention of Hopkins to include member sub-tracking devices as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery signature scheme can be enhanced with member sub-tracking devices so to avoid the forger to attack the system.

As for claim 9:

Examiner notes: Claim 9 recites "the group signature system of any one of claims 3, 6, 7, or 8". For examination purpose, it is assumed that claim 9 depends on claim 8.

The combination of Hopkins, Terao and Miyaji discloses the group signature system of any one of claims 3, 6, 7 or 8, wherein a finite field on an elliptic curve is used instead of said multiplicative group on a finite field. **(see Miyaji column 11 lines 50 to column lines 6 "An elliptic curve referred to here is a function that is generally expressed as $y^2 = x^3 + ax + b$, with E(GF(p)) denoting the set of points (x,y) that are elements of GF(p) and are present on the elliptic curve. The discrete logarithm problem based on the elliptic curve E(GE(p)) is as follows.**

Let Q and G be elements of E(GF(p)). The problem is to find a natural number d that satisfies the relationship ....This implies that the discrete logarithm problem based on an elliptic curve achieves the level of security similar to the discrete logarithm problem based on a finite field, with the smaller number of digits (for example, 160 bits in E(GF(p)) whereas 1024 bits in GF(p)). Note here that the present embodiment uses such an elliptic curve that p of the defining field GF(p) is equal to the order of G.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the modified-invention of Hopkins to include a finite field on an elliptic curve as taught by Miyaji because they are analogous in the group signature system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Miyaji in Hopkins so the conventional message recovery

signature scheme can be enhanced with a finite field on an elliptic curve so to avoid the forger to attack the system.

Claims 11, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins et al (US 2003/0120931 A1) hereinafter Hopkins, in view of Terao et al (US 2001/0009026 A1), hereinafter Terao.

As for claim 11:

Hopkins discloses a group signature device which forms a group signature system **(see Hopkins [0013] "a system and method for generating a group digital signature wherein each member of a group of authorized individuals must sign a message M to create a group digital signature S. ")** together with a group management device that discloses public information for common use throughout the system in a referenceable manner from other devices **(see Hopkins [0007] "the public key which is used to verify the digital signature. If many people need to verify a signer's digital signature, the associated public key must be available. A public key may be published or held in an on-line repository or directory where it is easily accessible. Although the public and private keys are mathematically related, it is extraordinarily difficult to derive the private key from knowledge of the public key.")** and a verification device**(see Hopkins [0006] "Digital signatures may be created and verified by cryptography. Digital signatures commonly use public key cryptography, which employs an algorithm using two different but mathematically related keys; one for creating a digital signature or encoding data, and another key for verifying a digital signature or decoding the message.")** that confirms

whether or not the signer of a group signature is a member registered in said group, and which creates a group signature that can prove that said signer is a member registered in said group **(see Hopkins [0004] "the signer somehow endorses the information to communicated by the document ")**, comprising: a member information storage means which stores a member certificate consisting of a first element and a second element, **(see Hopkins [0038] "this entity may perform such functions as receiving and storing partial signatures for a given message until a sufficient set is available for combining, receiving and storing different messages until signed, and verifying the validity of each group signature produced (using the public key) before issuing the signed message to the designated external recipient. ")** an encrypted data creation means which creates encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device, **(see Hopkins [0042] "the composite number n provides a modulus for encrypting and decrypting, and the prime numbers (or "primes") $p_1, p_2, \ldots p_k$ are referred to as factors of the modulus n. The primes $p_1, p_2, \ldots p_k$ must satisfy three general criteria in order to be used in a Multi-Prime cryptographic system. The primes $p_1, p_2, \ldots p_k$ must satisfy the criteria of being distinct, random, and suitable for use in the Multi-Prime cryptographic system. ")** a first converted data creation means which creates first converted data by converting said first element using a second random number and said public information, a second converted data creation means which creates second converted data by converting said first element using a third random number and said public information, **(see Hopkins**

[0017] "generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, 0 <=M< =n-1, n is a composite number formed from the product of a number k of distinct random prime factors $p_1.p_2.. . . . ..p_k$, k is an integer greater than 2, and $S= M^d$(mod n). ") a knowledge signature creation means which creates knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element, in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value **(see Hopkins [0017] "the method includes the steps of: a first individual in a group performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1; at least a second individual in the group performing a second partial digital signature subtask on the message M using a second individual private key to produce a second partial digital signature S_2; and combining the partial digital signature results including the results S_1 and S_2 to produce the group digital signature S corresponding to the message M.")**, and that information concerning said first element, said second element, and said signature key will not be divulged, **(see Terao [0051] "The proof data verification device 10 sends the authentication data 14 to the proof data generation device 11. The signature data generation means 15 and**

the presignature data generation means 16 in the proof data generation device 11 generate proof data (signature) from the received authentication data 14 and both the user unique identifying information (unique information for identifying the user) 17 and the access ticket 18 held in the proof data generation device 11, and sends the proof data thus generated back to the proof data verification device 10. The verification means 13 in the proof data verification device 10 verifies the signature, and if the verification is successful, the execution of program is permitted. ") and a signature output means which outputs as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message. **(see Terao [0055] "The proof data generation device 11 (constituted by both a program on a PC or a work station and an IC card) performs calculation on the basis of both user unique identifying information 17 and access ticket 18 and communicates with the proof data verification device 10 on the basis of the calculation. The user unique identifying information 17 is used in the course of this calculation, but if the information 17 leaks to the exterior, there arises a problem, so it is necessary that at least a part of the above program be protected by a defensive means such as an IC card or the like.")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include protecting the signature key (e.g. signature key will not be divulged) and signature output means (access ticket) as taught by Terao because they are analogous in the group signature

system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Terao in Hopkins so as not to permit stealing even by the user who is the legitimate holder thereof and that a proof hardware (e.g. IC card or board) having an anti-tamper characteristic be used.

As for claim 12:

Hopkins discloses a group signature program to be run on a computer to make the computer operate as a group signature device, which forms a group signature system **(see Hopkins [0013] "a system and method for generating a group digital signature wherein each member of a group of authorized individuals must sign a message M to create a group digital signature S. ")** together with a group management device that discloses public information for common use throughout the system in a referenceable manner from other devices **(see Hopkins [0007] "the public key which is used to verify the digital signature. If many people need to verify a signer's digital signature, the associated public key must be available. A public key may be published or held in an on-line repository or directory where it is easily accessible. Although the public and private keys are mathematically related, it is extraordinarily difficult to derive the private key from knowledge of the public key.")** and a verification device**(see Hopkins [0006] "Digital signatures may be created and verified by cryptography. Digital signatures commonly use public key cryptography, which employs an algorithm using two different but mathematically related keys; one for creating a digital signature or encoding data, and another key for verifying a digital signature or decoding the message.")**

that confirms whether or not the signer of a group signature is a member registered in said group, **(see Hopkins [0004] "the signer somehow endorses the information to communicated by the document ")** in order to create a group signature that can prove that said signer is a member registered in said group, comprising the processes of: a member information storage means storing a member certificate consisting of a first element and a second element; **(see Hopkins [0038] "this entity may perform such functions as receiving and storing partial signatures for a given message until a sufficient set is available for combining, receiving and storing different messages until signed, and verifying the validity of each group signature produced (using the public key) before issuing the signed message to the designated external recipient. ")** an encrypted data creation means creating encrypted data by encrypting said first element using a first random number and said public information disclosed by said group management device; **(see Hopkins [0042] "the composite number n provides a modulus for encrypting and decrypting, and the prime numbers (or "primes") p_1, p_2, . . . p_k are referred to as factors of the modulus n. The primes p_1, p_2, . . . p_k must satisfy three general criteria in order to be used in a Multi-Prime cryptographic system. The primes p_1, p_2, . . . p_k must satisfy the criteria of being distinct, random, and suitable for use in the Multi-Prime cryptographic system. ")** a first converted data creation means creating first converted data by converting said first element using a second random number and said public information; a second converted data creation means creating second converted data by converting said first element using a third random number and said

public information; **(see Hopkins [0017] "generating a group digital signature wherein each of a group of individuals may sign a message M to create a group digital signature S, wherein M corresponds to a number representative of a message, 0 <=M< =n-1, n is a composite number formed from the product of a number k of distinct random prime factors $p_1.p_2.. . . . ..p_k$, k is an integer greater than 2, and $S= M^d(mod\ n)$. ")** and a knowledge signature creation means creating knowledge signature data from a message to which a signature will be added, a fourth random number, said encrypted data, said first converted data, said second converted data, a signature key which is a private key to be used for the creation of a signature, said first element, and said second element, in such a manner that it can be proved that said encrypted data, said first converted data, and said second converted data have been created from the same value **(see Hopkins [0017] "the method includes the steps of: a first individual in a group performing a first partial digital signature subtask on a message M using a first individual private key to produce a first partial digital signature S_1; at least a second individual in the group performing a second partial digital signature subtask on the message M using a second individual private key to produce a second partial digital signature S_2; and combining the partial digital signature results including the results S_1 and S_2 to produce the group digital signature S corresponding to the message M.")**, and that information concerning said first element, said second element, and said signature key will not be divulged; **(see Terao [0051] "The proof data verification device 10 sends the authentication data 14 to the proof data generation device 11. The**

signature data generation means 15 and the presignature data generation means 16 in the proof data generation device 11 generate proof data (signature) from the received authentication data 14 and both the user unique identifying information (unique information for identifying the user) 17 and the access ticket 18 held in the proof data generation device 11, and sends the proof data thus generated back to the proof data verification device 10. The verification means 13 in the proof data verification device 10 verifies the signature, and if the verification is successful, the execution of program is permitted. ") and a signature output means outputting as a group signature said encrypted data, said first converted data, said second converted data, and said knowledge signature data, together with said message. **(see Terao [0055] "The proof data generation device 11 (constituted by both a program on a PC or a work station and an IC card) performs calculation on the basis of both user unique identifying information 17 and access ticket 18 and communicates with the proof data verification device 10 on the basis of the calculation. The user unique identifying information 17 is used in the course of this calculation, but if the information 17 leaks to the exterior, there arises a problem, so it is necessary that at least a part of the above program be protected by a defensive means such as an IC card or the like.")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Hopkins to include protecting the signature key (e.g. signature key will not be divulged) and signature output means (access ticket) as taught by Terao because they are analogous in the group signature

system and one of ordinary skill in the art would have been motivated to incorporate the teaching of Terao in Hopkins so as not to permit stealing even by the user who is the legitimate holder thereof and that a proof hardware (e.g. IC card or board) having an anti-tamper characteristic be used.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JASON LEE/
Examiner, Art Unit 2438

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438